

A Class of Linear Codes With Three Weights

Qiuyan Wang, Fei Li* and Dongdai Lin

Abstract

Linear codes have been an interesting subject of study for many years. Recently, linear codes with few weights have been constructed and extensively studied. In this paper, for an odd prime p , a class of three-weight linear codes over \mathbb{F}_p are constructed. The weight distributions of the linear codes are settled. These codes have applications in authentication codes, association schemes and data storage systems.

Index Terms

Association schemes, authentication codes, linear codes, secret sharing schemes.

I. INTRODUCTION

Throughout this paper, let p be an odd prime, and let $q = p^m$ for a positive integer $m > 2$. Let \mathbb{F}_q and \mathbb{F}_p denote the finite field with q elements and p elements, respectively.

An (n, M) code \mathcal{C} over \mathbb{F}_p is a subset of \mathbb{F}_p^n of size M . The vectors in \mathcal{C} are called codewords of \mathcal{C} . The third important parameter of a code \mathcal{C} , besides the length n and size M , is the minimum Hamming distance between codewords. The Hamming distance between two codewords $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ is defined to be the number of places where \mathbf{x} and \mathbf{y} differ. If the code \mathcal{C} is a k -dimensional subspace of \mathbb{F}_p^n with minimum (Hamming) distance d , it will be called an $[n, k, d]$ code over \mathbb{F}_p .

Let A_i be the number of codewords of weight i in \mathcal{C} of length n . The weight enumerator of \mathcal{C} is defined by

$$1 + A_1x + A_2x^2 + \cdots + A_nx^n.$$

For $0 \leq i \leq n$, the list A_i is called the weight distribution or weight spectrum of \mathcal{C} . A code \mathcal{C} is said to be a t -weight code if the number of nonzero A_i with $1 \leq i \leq n$ is equal to t . A great deal of research is devoted to the computation of the weight distribution of specific codes [1], [2], [3], [23], [22], [24], [25], [26], since it does give important information of both practical and theoretical significance.

Let $D = \{d_1, d_2, \dots, d_n\} \subseteq \mathbb{F}_q$. Let Tr denote the trace function from \mathbb{F}_q onto \mathbb{F}_p . A linear code of length n over \mathbb{F}_p is defined by

$$\mathcal{C}_D = \{(\text{Tr}(xd_1), \text{Tr}(xd_2), \dots, \text{Tr}(xd_n)) : x \in \mathbb{F}_q\},$$

and D is called the defining set of this code \mathcal{C}_D . This construction is proposed by Ding et al [11] and is generic in the sense that many known linear codes could be produced by selecting the defining set. If the defining set D is well chosen, some optimal linear codes with few weights can be obtained [10], [13], [20], [27], [30], [31], [32]. For more details, the readers are referred to [8], [15], [12], [17], [18].

In this correspondence, for $a \in \mathbb{F}_p^*$, we set

$$D_a = \{x \in \mathbb{F}_q^* : \text{Tr}(x) = a\} = \{d_1, d_2, \dots, d_{n_a}\},$$

The authors are supported by a National Key Basic Research Project of China (2011CB302400), National Natural Science Foundation of China (61379139), the ‘‘Strategic Priority Research Program’’ of the Chinese Academy of Sciences, Grant No. XDA06010701 and Foundation of NSSFC(No.13CTJ006).

Q. Wang is with the State Key Laboratory of Information Security, the Institute of Information Engineering, The Chinese Academy of Sciences, Beijing, China. Email: wangqiuyan@iie.ac.cn

F. Li is the corresponding author and with School of Statistics and Applied Mathematics, Anhui University of Finance and Economics, Bengbu City, Anhui Province, China. Email: cczxlf@163.com

D. Lin is with the State Key Laboratory of Information Security, the Institute of Information Engineering, The Chinese Academy of Sciences, Beijing, China. Email: ddlin@iie.ac.cn

and

$$\mathcal{C}_{D_a} = \{\mathbf{c}_x = (\text{Tr}(xd_1^2), \text{Tr}(xd_2^2), \dots, \text{Tr}(xd_{n_a}^2)) : d_i \in D_a, 1 \leq i \leq n_a, x \in \mathbb{F}_q\}. \quad (1.1)$$

The objective of this paper is to determine the weight distribution of the proposed linear codes. Results show that they are three-weight linear codes. The linear codes in this paper may yield associate schemes with framework introduced in [4] and can be employed to construct secret sharing schemes [29].

II. PRELIMINARIES

In this section, we present some basic notations and results of group characters and exponential sums. We start with the trace function. For $\alpha \in \mathbb{F}_{p^m}$, the *absolute trace* $\text{Tr}(\alpha)$ of α is defined by [21]

$$\text{Tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \dots + \alpha^{p^{m-1}}.$$

By definition, $\text{Tr}(\alpha)$ is always an element of \mathbb{F}_p .

An additive character χ of \mathbb{F}_q is a homomorphism from \mathbb{F}_q into the multiplicative group U of complex numbers of absolute value 1, that is, a mapping from \mathbb{F}_q into U with $\chi(x+y) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{F}_q$ [21]. For any $b \in \mathbb{F}_q$, the function

$$\chi_b(x) = \zeta_p^{\text{Tr}(bx)} \text{ for all } x \in \mathbb{F}_q,$$

defines an additive character of \mathbb{F}_q , where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$. For $b = 0$, the character $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$ and is called the *trivial* character of \mathbb{F}_q . All other additive character of \mathbb{F}_q are called *nontrivial*. For $b = 1$, the character χ_1 will be called the *canonical additive character* of \mathbb{F}_q . All additive characters of \mathbb{F}_q can be expressed in terms of χ_1 : $\chi_b(x) = \chi_1(bx)$ for all $x \in \mathbb{F}_q$ [21].

The orthogonal property of additive characters of \mathbb{F}_q which can be found in Theorem 5.4 in [21] is given by

$$\sum_{x \in \mathbb{F}_q} \chi(x) = \begin{cases} q, & \text{if } \chi \text{ is trivial,} \\ 0, & \text{if } \chi \text{ is nontrivial.} \end{cases} \quad (2.1)$$

Characters of the *multiplicative group* \mathbb{F}_q^* of \mathbb{F}_q are called *multiplicative characters* of \mathbb{F}_q . It is known that all characters of \mathbb{F}_q^* are given by

$$\psi_j(g^k) = \zeta_p^{2\pi\sqrt{-1}jk/(q-1)} \text{ for } k = 0, 1, \dots, q-2,$$

where $0 \leq j \leq q-2$ and g is a generator of \mathbb{F}_q^* [21]. For $j = (q-1)/2$, the multiplicative character $\psi_{(q-1)/2}$ is called the *quadratic character* of \mathbb{F}_q , and is denoted by η in this paper. It is convenient to extend the definition of η by setting $\eta(0) = 0$. With this definition, we have then

$$\sum_{x \in \mathbb{F}_q} \eta(x) = \sum_{x \in \mathbb{F}_q^*} \eta(x) = 0. \quad (2.2)$$

The quadratic Gauss sum $G(\eta, \chi_1)$ over \mathbb{F}_q is defined by

$$G(\eta, \chi_1) = \sum_{x \in \mathbb{F}_q} \eta(x) \chi_1(x),$$

and the quadratic Gauss sum $G(\bar{\eta}, \bar{\chi}_1)$ over \mathbb{F}_p is defined by

$$G(\bar{\eta}, \bar{\chi}_1) = \sum_{x \in \mathbb{F}_p} \bar{\eta}(x) \bar{\chi}_1(x),$$

where $\bar{\eta}$ and $\bar{\chi}_1$ denote the quadratic and canonical character of \mathbb{F}_p , respectively.

The explicit values of quadratic Gauss sums over a finite field are determined and given in the following lemma.

Lemma 1 (Theorem 5.15, [21]): Let the symbols be the same as before. Then

$$G(\eta, \chi_1) = (-1)^{(m-1)} \sqrt{-1}^{\frac{(p-1)^2 m}{4}} \sqrt{q},$$

and

$$G(\bar{\eta}, \bar{\chi}_1) = \sqrt{-1}^{\frac{(p-1)^2}{4}} \sqrt{p}.$$

Lemma 2 (Theorem 5.33, [21]): Let χ be a nontrivial additive character of \mathbb{F}_q , and let $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_q[x]$ with $a_2 \neq 0$. Then

$$\sum_{x \in \mathbb{F}_q} \chi(f(x)) = \chi(a_0 - a_1^2(4a_2)^{-1}) \eta(a_2) G(\eta, \chi).$$

Lemma 3 (Lemma 7, [14]): Let the symbols be the same as before. Then

- 1) if $m \geq 2$ is even, then $\eta(y) = 1$ for each $y \in \mathbb{F}_p^*$;
- 2) if m is odd, then $\eta(y) = \bar{\eta}(y)$ for each $y \in \mathbb{F}_p^*$.

Lemma 4: Let the symbols be the same as before. Then

$$\sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(byx^2) = \begin{cases} 0, & \text{if } m \equiv 1 \pmod{2}, \\ (p-1)\eta(b)G(\eta, \chi_1), & \text{if } m \equiv 0 \pmod{2}. \end{cases}$$

Proof: It follows from Lemma 2 that

$$\sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(byx^2) = \eta(b)G(\eta, \chi_1) \sum_{y \in \mathbb{F}_p^*} \eta(y).$$

Using Lemma 3, we get

$$\sum_{y \in \mathbb{F}_p^*} \eta(y) = \begin{cases} 0, & \text{if } m \equiv 1 \pmod{2}, \\ p-1, & \text{if } m \equiv 0 \pmod{2}. \end{cases}$$

Together with Lemma 1, we get this lemma. ■

III. THE LINEAR CODES WITH THREE WEIGHTS

In this section, we will present a class of linear codes with three weights over \mathbb{F}_p . The weight distributions of the class linear codes are also settled.

For $a \in \mathbb{F}_p$, set

$$D_a = \{x \in \mathbb{F}_q^* : \text{Tr}(x) = a\}.$$

If $a = 0$, the weight distribution of the code \mathcal{C}_{D_0} of (1.1) has been determined in [28]. Hence, we only consider the case $a \in \mathbb{F}_p^*$ in this paper.

It is well known that [21]

$$N_a = |\{x \in \mathbb{F}_q : \text{Tr}(x) = a, a \in \mathbb{F}_p\}| = p^{m-1}. \quad (3.1)$$

Then the length n_a of the code \mathcal{C}_{D_a} ($a \in \mathbb{F}_p^*$) of (1.1) satisfies

$$n_a = N_a = p^{m-1}.$$

Define

$$n_{(b,a)} = |\{x \in \mathbb{F}_q : \text{Tr}(x) = a \text{ and } \text{Tr}(bx^2) = 0\}|.$$

For any $b \in \mathbb{F}_q^*$, the Hamming weight $\text{wt}(\mathbf{c}_b)$ of the codeword \mathbf{c}_b of the code \mathcal{C}_{D_a} is given by

$$\text{wt}(\mathbf{c}_b) = N_a - n_{(b,a)} = p^{m-1} - n_{(b,a)}. \quad (3.2)$$

By the orthogonal property of additive characters, for $b \in \mathbb{F}_q^*$ we have

$$\begin{aligned}
n_{(b,a)} &= p^{-2} \sum_{x \in \mathbb{F}_q} \left(\sum_{y \in F_p} \zeta_p^{y \text{Tr}(bx^2)} \right) \left(\sum_{z \in F_p} \zeta_p^{z(\text{Tr}(x)-a)} \right) \\
&= p^{-2} \sum_{x \in \mathbb{F}_q} \left(1 + \sum_{y \in F_p^*} \zeta_p^{y \text{Tr}(bx^2)} \right) \left(1 + \sum_{z \in F_p^*} \zeta_p^{z(\text{Tr}(x)-a)} \right) \\
&= p^{m-2} + p^{-2} \sum_{y \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \text{Tr}(bx^2)} + p^{-2} \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{x \in \mathbb{F}_q} \zeta_p^{z \text{Tr}(x)} \\
&\quad + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \text{Tr}(bx^2) + z \text{Tr}(x) - za} \\
&= p^{m-2} + p^{-2} \sum_{y \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \text{Tr}(bx^2)} + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(byx^2 + zx)} \tag{3.3}
\end{aligned}$$

In the sequel, we will calculate $n_{(b,a)}$ for $a \in \mathbb{F}_p^*$.

Lemma 5: Let $b \in \mathbb{F}_q^*$. Then

$$\begin{aligned}
&\sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(byx^2 + zx) \\
&= \begin{cases} 0, & \text{if } m \equiv 1 \pmod{2} \text{ and } \text{Tr}(b^{-1}) = 0, \\ \eta(b)\eta(-\text{Tr}(b^{-1}))(-1)^{\frac{(p-1)(m+1)}{4}}(p-1)p^{\frac{m+1}{2}}, & \text{if } m \equiv 1 \pmod{2} \text{ and } \text{Tr}(b^{-1}) \neq 0, \\ \eta(b)(p-1)^2 G(\eta, \chi_1), & \text{if } m \equiv 0 \pmod{2} \text{ and } \text{Tr}(b^{-1}) = 0, \\ -\eta(b)(p-1)G(\eta, \chi_1), & \text{if } m \equiv 0 \pmod{2} \text{ and } \text{Tr}(b^{-1}) \neq 0, \end{cases}
\end{aligned}$$

where $G(\eta, \chi_1)$ is given in Lemma 1.

Proof: It follows from Lemmas 2 and 3 that

$$\begin{aligned}
& \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(byx^2 + zx) \\
&= \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \chi_1 \left(-\frac{z^2}{4by} \right) \eta(by) G(\eta, \chi_1) \\
&= \eta(b) G(\eta, \chi_1) \sum_{y_1 \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \chi_1 \left(-\frac{y_1 z^2}{b} \right) \eta \left(\frac{1}{4y_1} \right) \\
&= \eta(b) G(\eta, \chi_1) \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \chi_1 \left(-\frac{yz^2}{b} \right) \eta(y) \\
&= \eta(b) G(\eta, \chi_1) \sum_{z \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-yz^2 \text{Tr}(b^{-1})} \eta(y) \\
&= \begin{cases} \eta(b) G(\eta, \chi_1) \sum_{z \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} \eta(y), & \text{if } \text{Tr}(b^{-1}) = 0, \\ \eta(b) \eta(-\text{Tr}(b^{-1})) G(\eta, \chi_1) \sum_{z \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{yz^2 \text{Tr}(b^{-1})} \eta(yz^2 \text{Tr}(b^{-1})), & \text{if } \text{Tr}(b^{-1}) \neq 0. \end{cases} \\
&= \begin{cases} \eta(b) G(\eta, \chi_1) \sum_{z \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} \eta(y), & \text{if } \text{Tr}(b^{-1}) = 0, \\ \eta(b) \eta(-\text{Tr}(b^{-1})) G(\eta, \chi_1) \sum_{z \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} \zeta_p^y \eta(y), & \text{if } \text{Tr}(b^{-1}) \neq 0. \end{cases} \\
&= \begin{cases} 0, & \text{if } m \equiv 1 \pmod{2} \text{ and } \text{Tr}(b^{-1}) = 0, \\ \eta(b) \eta(-\text{Tr}(b^{-1})) (p-1) G(\eta, \chi_1) G(\bar{\eta}, \bar{\chi}_1) & \text{if } m \equiv 1 \pmod{2} \text{ and } \text{Tr}(b^{-1}) \neq 0, \\ \eta(b) (p-1)^2 G(\eta, \chi_1), & \text{if } m \equiv 0 \pmod{2} \text{ and } \text{Tr}(b^{-1}) = 0, \\ -\eta(b) (p-1) G(\eta, \chi_1), & \text{if } m \equiv 0 \pmod{2} \text{ and } \text{Tr}(b^{-1}) \neq 0. \end{cases}
\end{aligned}$$

Then the desired conclusion follows Lemma 1. ■

Lemma 6: Let

$$M = \{b \in \mathbb{F}_q^* : \eta(b) = -1 \text{ and } \text{Tr}(b) = 0\}$$

and

$$N = \{b \in \mathbb{F}_q^* : \eta(b) = 1 \text{ and } \text{Tr}(b) = 0\}.$$

Then

1)

$$|M| = \begin{cases} \frac{1}{2p}(q-p), & \text{if } m \equiv 1 \pmod{2}, \\ \frac{1}{2p}(q-p) + \frac{1}{2}(-1)^{\frac{(p-1)m}{4}}(p-1)p^{\frac{m-2}{2}}, & \text{if } m \equiv 0 \pmod{2}. \end{cases}$$

2)

$$|N| = \begin{cases} \frac{1}{2p}(q-p), & \text{if } m \equiv 1 \pmod{2}, \\ \frac{1}{2p}(q-p) - \frac{1}{2}(-1)^{\frac{(p-1)m}{4}}(p-1)p^{\frac{m-2}{2}}, & \text{if } m \equiv 0 \pmod{2}. \end{cases}$$

Proof: We only prove the first part of this lemma, since $|M| + |N| = p^{m-1} - 1$.

It follows from (2.1), (2.2), Lemmas 1 and 3 that

$$\begin{aligned}
|M| &= \frac{1}{2p} \sum_{x \in F_q^*} (1 - \eta(x)) \left(\sum_{y \in F_p} \zeta_p^{y \text{Tr}(x)} \right) \\
&= \frac{1}{2p} \sum_{x \in F_q^*} \left(1 - \eta(x) + \sum_{y \in F_p^*} \zeta_p^{y \text{Tr}(x)} - \sum_{y \in F_p^*} \eta(y) \zeta_p^{y \text{Tr}(x)} \right) \\
&= \frac{1}{2p} (q-1) - \frac{1}{2p} \sum_{x \in F_q^*} \eta(x) + \frac{1}{2p} \sum_{x \in F_q^*} \sum_{y \in F_p^*} \zeta_p^{y \text{Tr}(x)} - \frac{1}{2p} \sum_{x \in F_q^*} \sum_{y \in F_p^*} \eta(y) \zeta_p^{y \text{Tr}(x)} \\
&= \frac{1}{2p} (q-1) + \frac{1}{2p} \sum_{y \in F_p^*} \left(\sum_{x \in F_q} \zeta_p^{y \text{Tr}(x)} - 1 \right) - \frac{1}{2p} \sum_{y \in F_p^*} \eta(y) \sum_{x \in F_q^*} \eta(yx) \zeta_p^{y \text{Tr}(x)} \\
&= \frac{1}{2p} (q-1) - \frac{1}{2p} (p-1) - \frac{1}{2p} G(\eta, \chi_1) \sum_{y \in F_p^*} \eta(y) \\
&= \begin{cases} \frac{1}{2p} (q-p), & \text{if } m \equiv 1 \pmod{2}, \\ \frac{1}{2p} (q-p) + (-1)^{\frac{m(p-1)}{4}} \frac{1}{2} (p-1) p^{\frac{m-2}{2}}, & \text{if } m \equiv 0 \pmod{2}. \end{cases}
\end{aligned}$$

This completes the proof of the first conclusion of this lemma. ■

Lemma 7: For each $a \in \mathbb{F}_p^*$, let

$$M_a = \{x \in \mathbb{F}_q : \eta(x) = -1 \text{ and } \text{Tr}(x) = a\}.$$

Then

$$|M_a| = \begin{cases} \frac{q}{2p} - \frac{1}{2} \eta(-a) (-1)^{\frac{(m+1)(p-1)}{4}} p^{\frac{m-1}{2}}, & \text{if } m \equiv 1 \pmod{2}, \\ \frac{q}{2p} - \frac{1}{2} (-1)^{\frac{(p-1)m}{4}} p^{\frac{m-2}{2}}, & \text{if } m \equiv 0 \pmod{2}. \end{cases}$$

Proof: By (2.1), (2.2) and Lemma 1, for any $a \in \mathbb{F}_p^*$ we have

$$\begin{aligned}
|M_a| &= \frac{1}{2p} \sum_{x \in F_q} (1 - \eta(x)) \left(\sum_{y \in F_p} \zeta_p^{y(\text{Tr}(x)-a)} \right) \\
&= \frac{1}{2p} \sum_{x \in F_q} (1 - \eta(x)) + \frac{1}{2p} \sum_{x \in F_q} \sum_{y \in F_p^*} \zeta_p^{y(\text{Tr}(x)-a)} - \frac{1}{2p} \sum_{x \in F_q} \sum_{y \in F_p^*} \eta(y) \zeta_p^{y(\text{Tr}(x)-a)} \\
&= \frac{q}{2p} - \frac{1}{2p} \sum_{x \in F_q} \eta(x) + \frac{1}{2p} \sum_{y \in F_p^*} \sum_{x \in F_q} \zeta_p^{y(\text{Tr}(x)-a)} - \frac{1}{2p} \sum_{y \in F_p^*} \sum_{x \in F_q} \eta(y) \zeta_p^{y(\text{Tr}(x)-a)} \\
&= \frac{q}{2p} - \frac{1}{2p} \sum_{y \in F_p^*} \eta(y) \zeta_p^{-ya} \sum_{x \in F_q} \eta(yx) \zeta_p^{y \text{Tr}(x)} \\
&= \frac{q}{2p} - \frac{1}{2p} \eta(-a) G(\eta, \chi_1) \sum_{y \in F_p^*} \eta(-ay) \zeta_p^{-ya} \\
&= \begin{cases} \frac{q}{2p} - \frac{1}{2p} \eta(-a) G(\eta, \chi_1) G(\bar{\eta}, \bar{\chi}_1), & \text{if } m \equiv 1 \pmod{2}, \\ \frac{q}{2p} + \frac{1}{2p} G(\eta, \chi_1), & \text{if } m \equiv 0 \pmod{2}. \end{cases} \\
&= \begin{cases} \frac{q}{2p} - \frac{1}{2} (-1)^{\frac{(m+1)(p-1)}{4}} \eta(-a) p^{\frac{m-1}{2}}, & \text{if } m \equiv 1 \pmod{2}, \\ \frac{q}{2p} - \frac{1}{2} (-1)^{\frac{(p-1)m}{4}} p^{\frac{m-2}{2}}, & \text{if } m \equiv 0 \pmod{2}. \end{cases}
\end{aligned}$$

This completes the proof of this lemma. ■

Lemma 8: Let the symbols be the same as before. For each $b \in \mathbb{F}_q^*$, we have

1) if m is even, then

$$n_{(b,0)} = \begin{cases} p^{m-2} - (-1)^{\frac{(p-1)m}{4}}(p-1)\eta(b)p^{\frac{m-2}{2}}, & \text{if } \text{Tr}(b^{-1}) = 0, \\ p^{m-2}, & \text{if } \text{Tr}(b^{-1}) \neq 0; \end{cases}$$

2) if m is odd, then

$$n_{(b,0)} = \begin{cases} p^{m-2}, & \text{if } \text{Tr}(b^{-1}) = 0, \\ p^{m-2} + (-1)^{\frac{(p-1)(m+1)}{4}}(p-1)\eta(b)\eta(-\text{Tr}(b^{-1}))p^{\frac{m-3}{2}}, & \text{if } \text{Tr}(b^{-1}) \neq 0. \end{cases}$$

Proof: From the equation (3.3), we get

$$n_{(b,0)} = p^{m-2} + p^{-2} \sum_{y \in F_p^*} \sum_{x \in F_q} \zeta_p^{y \text{Tr}(bx^2)} + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \sum_{x \in F_q} \zeta_p^{y \text{Tr}(bx^2) + z \text{Tr}(x)}.$$

The desired conclusions then follow from Lemmas 4 and 5. ■

Next, we introduce the class of linear codes of (1.1) with three weights. For $a \in \mathbb{F}_p^*$, put

$$D_a = \{x \in \mathbb{F}_q^* : \text{Tr}(x) = a\}. \quad (3.4)$$

To get the weight distribution of \mathcal{C}_{D_a} constructed from the set D_a of (3.4), we need a number of auxiliary results.

Lemma 9: For any $a \in \mathbb{F}_p^*$, let

$$A = \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(byx^2 + zx)}.$$

Then for $b \in F_q^*$ we have

$$A = \begin{cases} 0, & \text{if } m \equiv 1 \pmod{2}, \text{Tr}(b^{-1}) = 0, \\ -(-1)^{\frac{(m+1)(p-1)}{4}}\eta(b)\eta(-\text{Tr}(b^{-1}))p^{\frac{m+1}{2}}, & \text{if } m \equiv 1 \pmod{2}, \text{Tr}(b^{-1}) \neq 0, \\ (-1)^{\frac{(p-1)^2}{2} \frac{m}{2}}\eta(b)(p-1)p^{\frac{m}{2}}, & \text{if } m \equiv 0 \pmod{2}, \text{Tr}(b^{-1}) = 0, \\ -(-1)^{\frac{(p-1)^2}{2} \frac{m}{2}}\eta(b)p^{\frac{m}{2}}, & \text{if } m \equiv 0 \pmod{2}, \text{Tr}(b^{-1}) \neq 0, \end{cases}$$

where $G(\eta, \chi_1)$ and $G(\bar{\eta}, \bar{\chi}_1)$ denote the square Gauss sum over \mathbb{F}_q and \mathbb{F}_p , respectively.

Proof: By Lemma 2, we have that

$$\begin{aligned} A &= \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \chi_1 \left(-\frac{z^2}{4by} \right) \eta(by) G(\eta, \chi_1) \\ &= \eta(b) G(\eta, \chi_1) \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \chi_1 \left(-\frac{yz^2}{b} \right) \eta \left(\frac{1}{4y} \right) \\ &= \eta(b) G(\eta, \chi_1) \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \chi_1 \left(-\frac{yz^2}{b} \right) \eta(y) \\ &= \eta(b) G(\eta, \chi_1) \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{y \in F_p^*} \zeta_p^{-yz^2 \text{Tr}(b^{-1})} \eta(y) \\ &= \begin{cases} \eta(b) G(\eta, \chi_1) \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{y \in F_p^*} \eta(y), & \text{if } \text{Tr}(b^{-1}) = 0, \\ \eta(b) \eta(-\text{Tr}(b^{-1})) G(\eta, \chi_1) \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{y \in F_p^*} \zeta_p^{yz^2 \text{Tr}(b^{-1})} \eta(yz^2 \text{Tr}(b^{-1})), & \text{if } \text{Tr}(b^{-1}) \neq 0. \end{cases} \\ &= \begin{cases} \eta(b) G(\eta, \chi_1) \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{y \in F_p^*} \eta(y), & \text{if } \text{Tr}(b^{-1}) = 0, \\ \eta(b) \eta(-\text{Tr}(b^{-1})) G(\eta, \chi_1) \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{y \in F_p^*} \zeta_p^y \eta(y), & \text{if } \text{Tr}(b^{-1}) \neq 0. \end{cases} \end{aligned}$$

For $a \in \mathbb{F}_p^*$, it is easy to check that

$$\sum_{z \in F_p^*} \zeta_p^{-za} = -1.$$

Then the results follow from Lemmas 1 and 3. ■

The following lemma follows directly from (3.3), Lemmas 4 and 9.

Lemma 10: Let the symbols be the same as before. Then for $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_q^*$

$$n_{(b,a)} = \begin{cases} p^{m-2}, & \text{if } \text{Tr}(b^{-1}) = 0, \\ p^{m-2} - (-1)^{\frac{(m+1)(p-1)}{4}} \eta(b) \eta(-\text{Tr}(b^{-1})) p^{\frac{m-3}{2}}, & \text{if } m \equiv 1 \pmod{2}, \text{Tr}(b^{-1}) \neq 0, \\ p^{m-2} - (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}} p^{\frac{m-2}{2}} \eta(b), & \text{if } m \equiv 0 \pmod{2}, \text{Tr}(b^{-1}) \neq 0. \end{cases}$$

By Lemmas 7 and 10, if $m > 2$, for $a \in \mathbb{F}_p^*$ we obtain

$$n_{(b,a)} \in \left\{ p^{m-2}, p^{m-2} - p^{\frac{m-2}{2}}, p^{m-2} + p^{\frac{m-2}{2}} \right\}$$

or

$$n_{(b,a)} \in \left\{ p^{m-2}, p^{m-2} - p^{\frac{m-3}{2}}, p^{m-2} + p^{\frac{m-3}{2}} \right\}$$

according as m is even or odd, respectively.

Now, for $a \in \mathbb{F}_p^*$ and the set D_a of (3.4), we are ready to determine the weight distribution of the code \mathcal{C}_{D_a} of (1.1).

TABLE I: The weight distribution of the codes of Theorem 11

Weight	Multiplicity
0	1
$(p-1)p^{m-2}$	$p^{m-1} - 1$
$(p-1)p^{m-2} + p^{\frac{m-3}{2}}$	$\frac{1}{2}(p-1)(p^{m-1} + p^{\frac{m-1}{2}})$
$(p-1)p^{m-2} - p^{\frac{m-3}{2}}$	$\frac{1}{2}(p-1)(p^{m-1} - p^{\frac{m-1}{2}})$

Theorem 11: For $a \in \mathbb{F}_p^*$, if m is odd, then the linear code \mathcal{C}_{D_a} over \mathbb{F}_p has parameters $[p^{m-1}, m]$ and weight distribution in Table I.

Proof: If $m \equiv 1 \pmod{2}$, by Lemma 7, for $a \in \mathbb{F}_p^*$ we have that

$$\begin{aligned} |M_a| &= |\{x \in F_q : \eta(x) = -1 \text{ and } \text{Tr}(x) = a\}| \\ &= \frac{q}{2p} - \frac{1}{2p} \eta(-a) G(\eta, \chi_1) G(\bar{\eta}, \bar{\chi}_1). \end{aligned}$$

Let

$$\begin{aligned} \overline{M}_a &= \{x \in F_q : \eta(x) = 1 \text{ and } \text{Tr}(x) = a\}, \\ S &= \{x \in F_q : \eta(x) = -1 \text{ and } \eta(\text{Tr}(x)) = 1\}, \end{aligned}$$

and

$$\overline{S} = \{x \in F_q : \eta(x) = 1 \text{ and } \eta(\text{Tr}(x)) = -1\}.$$

Notice that half of the elements in F_p^* are squares. Hence we get

$$|S| = \frac{p-1}{2} \left(\frac{q}{2p} - \frac{1}{2p} \eta(-1) G(\eta, \chi_1) G(\bar{\eta}, \bar{\chi}_1) \right)$$

and

$$|\overline{S}| = \frac{p-1}{2} \left(p^{m-1} - \frac{q}{2p} + \frac{1}{2p} \eta(-1)(-1) G(\eta, \chi_1) G(\bar{\eta}, \bar{\chi}_1) \right).$$

Set

$$T = \{x \in F_q : \eta(x)\eta(\text{Tr}(x)) = -1\},$$

and

$$\overline{T} = \{x \in F_q : \eta(x)\eta(\text{Tr}(x)) = 1\}.$$

By definition, we obtain

$$|T| = |S| + |\overline{S}| = \frac{p-1}{2} \left(p^{m-1} - \frac{1}{p} \eta(-1) G(\eta, \chi_1) G(\overline{\eta}, \overline{\chi}_1) \right).$$

and

$$|\overline{T}| = p^m - p^{m-1} - |T| = \frac{p-1}{2} \left(p^{m-1} + \frac{1}{p} \eta(-1) G(\eta, \chi_1) G(\overline{\eta}, \overline{\chi}_1) \right)$$

Note that $\eta(-1) = (-1)^{\frac{p-1}{2}}$ and $G(\eta, \chi_1) G(\overline{\eta}, \overline{\chi}_1) = (-1)^{\frac{(m+1)(p-1)}{4}} p^{\frac{m+1}{2}}$. Then the weight distribution of Table I follows from (3.2) and Lemma 10. It can be easily checked that $\text{wt}(\mathbf{c}_b) > 0$ for $b \in \mathbb{F}_q^*$. Hence, the dimension of this code \mathcal{C}_{D_a} of Theorem 11 is equal to m . ■

Example 1: Let $(p, m, a) = (5, 3, 1)$. Then the corresponding code \mathcal{C}_{D_1} has parameters $[25, 3, 19]$ and weight enumerator $1 + 40x^{19} + 24x^{20} + 60x^{21}$. Remark that this code is almost optimal, since an optimal $[25, 3]$ code has minimum distance 20.

Example 2: Let $(p, m, a) = (3, 3, 1)$. Then the corresponding code \mathcal{C}_{D_1} has parameters $[9, 3, 5]$ and weight enumerator $1 + 6x^5 + 8x^6 + 12x^7$. Remark that this code is almost optimal, since an optimal $[9, 3]$ code has minimum distance 6.

TABLE II: The weight distribution of the codes of Theorem 12

Weight	Multiplicity
0	1
$(p-1)p^{m-2}$	$p^{m-1} - 1$
$(p-1)p^{m-2} + p^{\frac{m-2}{2}}$	$\frac{1}{2}(p-1)(p^{m-1} + p^{\frac{m-2}{2}})$
$(p-1)p^{m-2} - p^{\frac{m-2}{2}}$	$\frac{1}{2}(p-1)(p^{m-1} - p^{\frac{m-2}{2}})$

Theorem 12: For $a \in \mathbb{F}_p^*$, if m is even, then the linear code \mathcal{C}_{D_a} over \mathbb{F}_p has parameters $[p^{m-1}, m]$ and weight distribution in Table II.

Proof: If $m \equiv 0 \pmod{2}$, by Lemma 6, we have

$$\begin{aligned} |M| &= |\{b \in \mathbb{F}_q^* : \eta(b) = -1 \text{ and } \text{Tr}(b) = 0\}| \\ &= \frac{1}{2p}(q-p) + \frac{1}{2p}(-1)^{\frac{m(p-1)}{4}}(p-1)p^{\frac{m}{2}}. \end{aligned}$$

Let

$$\begin{aligned} \overline{M} &= \{b \in \mathbb{F}_q^* : \eta(b) = -1 \text{ and } \text{Tr}(b) \neq 0\}, \\ N &= \{b \in \mathbb{F}_q^* : \eta(b) = 1 \text{ and } \text{Tr}(b) = 0\}, \end{aligned}$$

and

$$\overline{N} = \{b \in \mathbb{F}_q^* : \eta(b) = 1 \text{ and } \text{Tr}(b) \neq 0\}.$$

By definition, we know

$$|N| = p^{m-1} - 1 - |M|.$$

Since $|\{b \in \mathbb{F}_q^* : \eta(b) = -1\}| = (q-1)/2$, we get

$$|\overline{M}| = \frac{1}{2}(q-1) - |M| = \frac{p-1}{2} \left(p^{m-1} - (-1)^{\frac{m(p-1)}{4}} p^{\frac{m-2}{2}} \right),$$

and

$$|\overline{N}| = \frac{1}{2}(q-1) - |N| = \frac{p-1}{2} \left(p^{m-1} + (-1)^{\frac{(p-1)m}{4}} p^{\frac{m-2}{2}} \right).$$

The weight distribution of Table II follows from (3.2) and Lemma 10. The dimension of the code \mathcal{C}_{D_a} of Theorem 12 equals m , since $\text{wt}(\mathbf{c}_b) > 0$ for $b \in \mathbb{F}_q^*$. ■

Example 3: Let $(p, m, a) = (5, 4, 1)$. Then the corresponding code \mathcal{C}_{D_1} has parameters $[125, 4, 95]$ and weight enumerator $1 + 240x^{95} + 124x^{100} + 260x^{105}$.

Example 4: Let $(p, m, a) = (3, 4, 1)$. Then the corresponding code \mathcal{C}_{D_1} has parameters $[27, 3, 15]$ and weight enumerator $1 + 24x^{15} + 26x^{18} + 30x^{21}$.

IV. CONCLUDING REMARKS

In this paper, we present a class of linear codes with three weights. There is a survey on three-weight codes in [11]. A number of three-weight codes were constructed in [5], [6], [7], [8], [12], [14], [15], [17], [18], [27], [28], [31], [32]. We did not find the parameters of the class of linear codes \mathcal{C}_{D_a} ($a \in \mathbb{F}_p^*$) in this paper in these references.

Let w_{\min} and w_{\max} denote the minimum and maximum nonzero weight of a linear code \mathcal{C} . As stated in [29], the linear code \mathcal{C} can be employed to construct a secret sharing scheme with interesting access structures if $w_{\min}/w_{\max} > p-1/p$.

Let $m \equiv 1 \pmod{2}$ and $m > 3$. Then for the linear code \mathcal{C}_{D_a} ($a \neq 0$) of Theorem 11, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{(p-1)p^{m-2} - p^{\frac{m-3}{2}}}{(p-1)p^{m-2} + p^{\frac{m-3}{2}}} > \frac{p-1}{p}.$$

Let $m \equiv 0 \pmod{2}$ and $m > 2$. Then for the linear code \mathcal{C}_{D_a} ($a \neq 0$) of Theorem 12, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{(p-1)p^{m-2} - p^{\frac{m-2}{2}}}{(p-1)p^{m-2} + p^{\frac{m-2}{2}}} > \frac{p-1}{p}.$$

Hence, the linear codes in this paper satisfy $w_{\min}/w_{\max} > (p-1)/p$ if $m \geq 6$, and can be used to get secret sharing schemes with interesting access structures.

REFERENCES

- [1] L. D. Baumert and R. J. McEliece, Weights of irreducible cyclic codes, *Inf. Contr.*, vol. 20, no. 2, pp. 158-175, 1972.
- [2] L. D. Baumert and J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, *DSN Progr. Rep.*, vol. 16, pp. 128-131, 1973.
- [3] N. Boston and G. McGuire, The weight distribution of cyclic codes with two zeros and zeta functions, *J. Symbolic Comput.*, vol. 45, no. 7, pp. 723-733, 2010.
- [4] A. R. Calderbank, J. M. Goethals, "Three-weight codes and association schemes," *Philips J. Res.* **39**, (1984), 143C152.
- [5] S.-T. Choi, J.-Y. Kim, J.-S. No, and H. Chung, "Weight distribution of some cyclic codes," in *Proc. Int. Symp. Inf. Theory*, (2012), 2911-2913.
- [6] B. Courteau, J. Wolfmann, "On triple-sum-sets and two or three weights codes," *Discret. Math.*, **50**, (1984), 179-191.
- [7] C. Ding, "A class of three-weight and four-weight codes," in: C. Xing, et al. (Eds.), *Proc. of the Second International Workshop on Coding Theory and Cryptography*, in: *Lecture Notes in Computer Science*, vol. 5557, Springer Verlag, (2009), 34-42.
- [8] C. Ding, "Linear codes from some 2-designs," *IEEE Trans. Inf. Theory*, **61**(6), 2015, 3265-3275.
- [9] C. Ding, J. Luo, H. Niederreiter, "Two-weight codes punctured from irreducible cyclic codes," in: Y. Li, et al. (Eds.), *Proceedings of the First Workshop on Coding and Cryptography*, World Scientific, Singapore, (2008), 119-124.
- [10] C. Ding and H. Niederreiter, "Cyclotomic linear codes of order 3," *IEEE Trans. Inf. Theory*, **53**(6), 2007, 2274-2277.
- [11] C. Ding, C. Li, N. Li, and Z. Zhou, "Three-Weight Cyclic Codes and Their Weight Distributions," submitted for publication.
- [12] C. Ding, J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Math.*, **313**(4), (2013), 434-446, .
- [13] C. Ding and J. Yin, "Algebraic constructions of constant composition codes," *IEEE Trans. Inf. Theory*, **51**(4), (2005), 1585-1589. C. Ding, Y. Gao, Z. Zhou, "Five Families of Three-Weight Ternary Cyclic Codes and Their Duals," *IEEE Trans. Inf. Theory*, **59**(12), 2013, 7940-7946.
- [14] K. Ding, C. Ding, "A class of two-weight and three-weight codes and their applications in secret sharing," arXiv:1503.06512v1.
- [15] K. Ding, C. Ding, "Bianry linear codes with three weights," *IEEE Commu. Lett.*, **18**(11), (2014), 1879-1882.
- [16] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge: Cambridge University Press, 2003.
- [17] C. Li, Q. Yue, and F. Li, "Weight distributions of cyclic codes with respect to pairwise coprime order elements, *Finite Fields Appl.*, **28**, (2014), 94- 114.

- [18] C. Li, Q. Yue, and F. Li, Hamming weights of the duals of cyclic codes with two zeros, *IEEE Trans. Inf. Theory*, **60**(7), (2014), 3895–3902.
- [19] C. Li, Q. Yue, and F. W. Fu, “Complete weight enumerators of some cyclic codes,” *Des. Codes Cryptogr.*, DOI 10.1007/s10623-015-0091-5, 2015.
- [20] C. Li, Q. Yue, “Weight Distributions of Two Classes of Cyclic Codes With Respect to Two Distinct Order Elements,” *IEEE Trans. Inf. Theory*, **60**(1), (2014), 296–303.
- [21] R. Lidl, H. Niederreiter, *Finite Fields*. Cambridge University Press, New York, (1997)
- [22] McGuire, On three weights in cyclic codes with two zeros, *Finite Fields Appl.*, vol. 10, pp. 97-104, 2004.
- [23] R. J. McEliece, A class of two-weight codes, Jet Propulsion Laboratory Space Program Summary 37-41, vol. IV, pp. 264-266, 1966.
- [24] R. Schoof, Families of curves and weight distribution of codes, *Bull. Amer. Math. Soc.*, vol. 32, no. 2, pp. 171C183, 1995.
- [25] A. Sharma and G. K. Bakshi, The weight distribution of some irreducible cyclic codes, *Finite Fields Appl.*, vol. 18, no. 1, pp. 144C159, 2012.
- [26] G. Vega, The weight distribution of an extended class of reducible cyclic codes, *IEEE Trans. Inform. Theory*, vol. 58, no. 7, pp. 4862-4869, July 2012.
- [27] Q. Wang, K. Ding, R. Xue, “Binary linear codes with two weights”, *IEEE Commun. Lett.* **19**(7), (2015).
- [28] S. Yang, Z. Yao, “Complete Weight Enumerators of a Family of Three-Weight Linear Codes,” arxiv: 1509.01371v1
- [29] J. Yuan and C. Ding, “Secret sharing schemes from three classes of linear codes,” *IEEE Trans. Inf. Theory*, **52**(1), (2006), 206–212.
- [30] Z. Zhou, C. Ding, “Seven Classes of Three-Weight Cyclic Codes,” *IEEE Trans. Commun.*, **61**(10), (2013), 4120–4126.
- [31] Z. Zhou, C. Ding, “A class of three-weight cyclic codes,” *Finite Fields Appl.*, **25**, (2014), 79–93.
- [32] Z. Zhou, N. Li, C. Fan, T. Helleseht, “Linear codes with two or three weights from quadratic bent functions,” arXiv:1505.06830